

CLAIMS

What is claimed is:

1 1. A method comprising:
2 loading port authentication firmware instructions in a suppliant system; and
3 authenticating a network port hosted by an authenticator system to which the
4 suppliant system is linked via execution of the port authentication firmware
5 instructions on the suppliant system.

1 2. The method of claim 1, wherein the network port is authenticated during a
2 pre-boot phase.

1 3. The method of claim 2, further comprising loading an operating system image
2 into the suppliant system over a network that is accessed via the network port that
3 is authenticated.

1 4. The method of claim 1, wherein the network port is authenticated during an
2 operating system (OS)-runtime phase.

1 5. The method of claim 4, wherein network port authentication is performed by
2 executing the port authentication firmware using a hidden execution mode that is
3 transparent to an operating system running on the suppliant system during the OS-
4 runtime phase

1 6. The method of claim 5, wherein the hidden execution mode is a system
2 management mode (SMM).

1 7. The method of claim 6, wherein the firmware instructions are embodied as
2 one or more SMM handlers.

1 8. The method of claim 7, further comprising:
2 asserting one of an SMI (system management interrupt) or PMI (Processor
3 Management Interrupt) on a processor of the suppliant on a periodic basis;
4 dispatching said one or more SMM handlers to handle the SMI or PMI
5 event via operations including,
6 determining if a network port needs to be authenticated; and, in
7 response thereto,
8 authenticating the network port.

1 9. The method of claim 1, wherein port authentication is performed using the
2 EAPOL (extensible authentication protocol over local area network) protocol.

1 10. The method of claim 1, wherein the port is authenticated using an
2 access/challenge scheme.

1 11. The method of claim 10, wherein the access/challenge scheme employs a
2 Transport Layer Security (TLS) challenge response in which authentication is
3 determined based on credentials provided by the suppliant system.

1 12. The method of claim 11, wherein the TLS challenge response employs
2 credentials stored in a Trusted Platform Module (TPM), and wherein the method
3 further comprises retrieving the credentials from the TPM.

1 13. The method of claim 1, wherein a determination of whether a port is
2 authenticated is made by an authentication server that is linked in communication
3 with the authenticator system.

1 14. The method of claim 1, further comprising providing an callable interface via
2 which a port authentication process can be invoked.

1 15. A method comprising:
2 executing instructions comprising port authentication code via a baseboard
3 management controller (BMC) in a supplicant system to perform port authentication
4 of a authenticator system port to which the supplicant system is linked in
5 communication.

1 16. The method of claim 15, wherein the port authentication code is stored in a
2 non-volatile storage device coupled to the BMC, the method further comprising
3 loading the port authentication code into the BMC for execution.

1 17. The method of claim 15, wherein the port authentication is performed during
2 an operating system runtime phase.

1 18. A method comprising:
2 retrieving authentication credentials pertaining to a supplicant system during a
3 pre-boot phase of the supplicant system;
4 passing the authentication credentials to an operating system running on the
5 supplicant system during an operating system runtime phase; and
6 authenticating a network port to which the supplicant system is connected via
7 use of the authentication credentials.

1 19. The method of claim 18, wherein the operating system is compliant with the
2 IEEE 802.1x port-based network access control standard and authenticates the
3 network port via an 802.1x authentication protocol.

1 20. The method of claim 19, wherein the network port is authenticated using a
2 Transport Layer Security (TLS) challenge response in which authentication is
3 determined based on the authentication credentials.

1 21. A machine-readable media on which firmware instructions are stored, which
2 when executed by a supplicant system perform operations including:
3 authenticating a network port hosted by an authenticator system to which the
4 supplicant system is linked.

1 22. The machine-readable media of claim 21, wherein the media comprises a
2 firmware storage device.

1 23. The machine-readable media of claim 21, wherein the firmware instructions
2 comprise at least one system management mode (SMM) handler that is executed by
3 a processor of the supplicant system while operating in SMM.

1 24. The machine-readable media of claim 21, wherein the network port is
2 authenticated during a pre-boot phase of the supplicant system.

1 25. A supplicant system comprising:
2 a processor;
3 a network interface, coupled to the processor; and

4 a flash device coupled to the processor, having firmware instructions stored
5 therein that when executed on the processor perform operations including:
6 authenticating a network port hosted by an authenticator system to
7 which the suppliant system is linked in communication via the network
8 interface.

1 26. The suppliant system of claim 25, further comprising a trusted platform
2 module coupled to the processor, to store authentication credentials employed for
3 authenticating the network port.

1 27. The suppliant system of claim 25, wherein the processor includes a hidden
2 execution mode and the network port is authenticated during an operating system
3 runtime phase via execution of firmware instructions under the hidden execution
4 mode.

1 28. A suppliant system comprising:
2 a baseboard management controller (BMC);
3 a network interface, coupled to the baseboard management controller;
4 and
5 machine-executable instructions stored on the suppliant system, which when
6 executed on the BMC perform operations including:
7 authenticating a network port hosted by an authenticator system to which the
8 suppliant system is linked in communication via the network interface.

1 29. The suppliant system of claim 28, further comprising a trusted platform
2 module coupled to the BMC, to store authentication credentials employed for
3 authenticating the network port.

- 1 30. The suppliant system of claim 28, wherein the machine-executable
- 2 instructions are stored in one of the BMC or a non-volatile storage device coupled to
- 3 that BMC.